

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

1. I, Brian Judd, a Task Force Officer with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows
2. Your affiant has been a Sworn Law Enforcement officer for 19 years with the Sheboygan County Sheriff's Office, and currently holds the rank of Detective. I have been a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI) for 8 years.
3. In my position, since 2009, my primary duty has been to conduct Forensic Examination of Computers and Digital media. I have also been trained in conducting Peer to Peer child exploitation investigations. I am currently assigned to the FBI Milwaukee Division Child Exploitation Task Force (CETF). I am charged with conducting investigations of violations of federal law including the receipt, possession, distribution, and production of child pornography. I have gained experience in the conduct of such investigations through prior investigations, formal training, and in consultation with other members of the CETF regarding these matters.
4. As part of my duties with CETF, I have received TFO/Special Deputy United States Marshal designation authorizing me to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. Thus, I am considered a federal law enforcement officer able to present and execute federal search warrants.

5. **Training** : Computer Forensics with FRED by Digital Intelligence, EnCase V6 / Forensic Software Training, 2010 Wisconsin Computer Crimes Investigators Conference, 2012 Wisconsin Computer Crimes Investigators Conference, Gnutella Peer 2 Peer Training FBI Cyber Crimes Task Force, Internet Evidence Finder Training FBI Cyber Crimes Task Force, Cellebrite Physical Analyzer / iPhone acquisition Tool Training FBI Cyber Crimes Task Force, Ongoing Forensic training with FBI Computer Forensic Examiners, Katana Forensics Lantern IOS forensic training by Jim Luty, Katana Forensics, Lantern Certified Examiner (Mobil Forensics), EnCase V7 Computer Forensics I, EnCase V7 Computer Forensics II, ICAC Ares Investigations, ICAC eMule Investigations, FBI DOJ Innocent Images Online Basic Training Program, (Gigatribe, OS triage), Cellebrite Certified Physical Analyst, Cyber Investigations, GPS Interrogation National White Collar Crime Center, FBI BitTorrent Investigations, Cell Phone Chip off Training.
6. The facts contained in this affidavit are known to me through my personal knowledge, training, official reports and experience, and through information provided to me by other law enforcement officers, who have provided information to me during the course of their official duties and whom I consider to be truthful and reliable. Some of the information was provided in response to administrative subpoenas and I believe this information to be reliable.
7. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of: 18 U.S.C. § 2252A(a)(2) and (a)(5)(B) and

(b)(2) (receipt and possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography), are located within 310 Wyldewood Drive, Oshkosh, WI, (the SUBJECT PREMISES). It is further believed that Martin Mckeever who resides at that address is the responsible party for these activities.

8. I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, as further described in Attachments A and B, incorporated herein by reference, which is located in the Eastern District of Wisconsin. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer, cell phone and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime. I further seek permission to search the items such as computer and cell phone seized from the subject premises.
9. The statements contained in this affidavit are based in part on: information provided by Law Enforcement officers in the State of Wisconsin and FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI

agents/analysts and computer forensic professionals; and my experience, training and background as a Task Force Officer (TFO) with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

RELEVANT STATUTES

10. This investigation concerns alleged violations of: 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt, Transportation, and Distribution, and Conspiracy to Receive, Transport, and Distribute, Child Pornography; and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Possession and Access, or Attempted Access, with Intent to View Child Pornography.
- a. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and
 - b. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any

means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

11. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DEFINITIONS

12. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

- a. "Cellular telephone" or "cell phone" means a hand held wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information

indicating where the cell phone was at particular times.

- b. "Computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."
- c. "Computer Server" or "Server," is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.
- d. "Computer hardware" means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including,

but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- e. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- g. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software

or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

- h. “Electronic storage devices” includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB “thumb drives”). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).
- i. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- j. “Internet Service Providers” (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of

connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

- k. “An Internet Protocol address” (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term IP addresses, while other computers have dynamic—that is, frequently changed IP addresses.
- l. “Hash Value” refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a “digital fingerprint” for data. If the data is changed, even very slightly (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a

known file, it means that the digital photo is an exact copy of the known file.

- m. "Media Access Control" (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.
- n. "Minor" means any person under the age of eighteen years.
- o. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or

readouts from any magnetic, electrical or electronic storage device).

- p. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.
- q. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image.
- r. "ARIN" is the American Registry for Internet Numbers, which manages the distribution of Internet number resources including IPv4 and IPv6 address space for Canada, the United States, and may Caribbean and North Atlantic Islands.

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

13. I have consulted in this matter with lay persons and law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. Based on my training and experience and speaking with other forensic examiners who have also received specialized training as a forensic computer, cellular telephone, and other electronic storage device examiner, I know to properly retrieve and analyze electronically stored (computer) data, and to insure accuracy and completeness of such data and to prevent loss of the data either from accidental or

programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To affect such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer(s) hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

14. Based on my knowledge, training, and experience, I know that computer and other electronic device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects.
 - a. The objects themselves may be instrumentalities used to commit the crime;
 - b. the objects may have been used to collect and store information about crimes (in the form of electronic data); and
 - c. the objects may be contraband or fruits of the crime.

15. I submit that if a computer or other electronic storage device is found on the premises,

there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone or tablet device) the device may also contain a record of deleted data.
- b. Wholly apart from user-generated files, electronic storage device storage media in particular, computer(s) internal hard drives contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from

operating system or application operation, and file system data structures.

Electronic storage device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.
- d. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when.

16. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

- a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has

been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

- b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was

remotely accessed, thus inculcating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either inculcate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For

example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.
- d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user(s) knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

17. Based upon my knowledge, training and experience, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

- a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.
- b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

- c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

18. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

19. I know that when an individual uses a computer to commit crimes involving child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of

the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain: data that is evidence of how the electronic storage device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

CHATTING APPLICATIONS

20. Kik is a smartphone messenger application that lets users connect with their friends and the world around them through chat. Users can send text, pictures, videos and more – all within the app. Kik is available for download through the iOS App Store and the Google Play store on most iOS (iPhone, iPod, iPad), Android (including Kindle Fire) and Windows 7 devices. Users may also be using Kik on their Symbian-based or BlackBerry 4.6-7 phone, however, as of May 2014, it's no longer possible to download or register new accounts on these devices. Kik is free to download and uses an existing Wi-Fi connection or data plan to send and receive messages.
21. Mega provides user-controlled encrypted cloud storage and chat through standard web browsers and dedicated apps for mobile devices. Users can upload files from smartphones, tablet, or computers then search, store, download, stream, view, share, rename or delete files any time, from any device, anywhere. Mega also provides end-to-end user-encrypted Mega video chat Users can also easily add files to a chat from

their Mega cloud drive. Mega provides 50 GB free storage for all registered users and offers paid plans with much higher limits.

22. Because Mega is a New Zealand Company, it takes the position that it is not subject to U.S. legal process unless such process originates through the Mutual Assistance Process in New Zealand. Accordingly, the processes set forth in Title 18, United States Code, Sections 2703(a), (b), and (c), and Rule 41 of the Federal Rules of Criminal Procedure cannot compel Mega to produce the contents of Mega account. Mega, however, routinely cooperates with law enforcement agencies through the New Zealand, Department of Internal Affairs (DIA), and in accordance with its policies and procedures, will voluntarily preserve and provide the contents of a user's account to New Zealand, DIA, who may then forward the account information to foreign agencies.

ONLINE COVERT EMPLOYEES

23. Online Covert Employee (OCE1) is a Federal Bureau of Investigation employee conducting online investigations in an undercover capacity. I know their true identity and they have provided reliable information in the past.
24. Online Covert Employee (OCE2) is a Winnebago County Sheriff's Office employee conducting online investigations in an undercover capacity. I know their true identity and they have provided reliable information in the past.

DETAILS OF THE INVESTIGATION

25. OCE1 times are listed in Eastern Daylight Savings Time.

26. OCE2 times are listed in Central Standard Time.

27. On August 18, 2019, OCE-10174 (OCE1) began communicating with an individual via Mega private messenger with the display name Alex Cross and subscriber name SlackerMaster2k@yahoo.com. SlackerMaster2k@yahoo.com uploaded numerous nude images of teenage boys directly into the chat. Historically, this subscriber was a member of a Kik forum that the OCE1 was also a member of entitled "Boys in Motion". This subscriber on Kik had a display name of Alex Cross and username of Alex_chross. At one point on Kik, this user uploaded a live photograph of their legs and in the background was a name plate could be observed that displayed "Marty Mckeever". In the Kik chats, this user disclosed that they reside in Wisconsin. OCE1 stated that he was chatting with Kik user Alex_chross and knew him based on their conversations to also be the Mega user with the display name, Alex Cross (slackermaster2k@yahoo.com).

28. On August 26, 2019, at 1906hrs, Mega user slackermaster2k@yahoo.com sent an image to OCE1 of a teenage male whom is laying on a bed with an erect penis and second individual's hand near it to OCE1. At 2233hrs, an image of an unclothed teenager covering their genitals is sent to OCE1. Based on the photos, it is difficult to determine age.

29. On August 29, 2019, at 1324hrs, Mega user slackermaster2k@yahoo.com sent an image to OCE1 of an approximately 12-14 year old male pulling his pants away from his body exposing his erect penis.

30. On August 29, 2019, at 1526hrs, Mega user slackermaster2k@yahoo.com uploaded

Mega link <https://mega.nz/#F!nnZSIa4D!OXYq0QYjJKiIX0fSZ7DMFw> to the private message with OCE1. The link pointed to a publicly accessible folder titled "The Goodies" and contained 681 files. OCE1 accessed the link and downloaded 35 videos at that time. Mega user slackermaster2k@yahoo.com commented, "Not sure which this is:" OCE1 responded, "Omg thank you!!!" Mega user slackermaster2k@yahoo.com responded, "Anytime."

31. On August 30, 2019, at 0859hrs, OCE1 responded, "So far 261,919, and 179 making me cum haha." OCE1 was referencing the link he was sent. The files 261, 919 and 179 were contained in "The Goodies" link and contained teen age boys engaged in sex acts. At 0954hrs, Mega user slackermaster2k@yahoo.com responded, "Mmm" "I'd LOVE to watch u cum." At 1053 hrs, Mega user slackermaster2k@yahoo.com, posted, "Cole wants me to come ohio..lol..do u think he is really that young?" OCE1 responds, "I know he was trying to get me there too," "I don't know," "Not sure who to trust on here really besides you and couple others we have history with haha," "Whats he saying," "Ask what his dad does," "He told me he's a cop, the dad." At 1302hrs, Mega user slackermaster2k@yahoo.com responds, " Yikes, Did you see his 'brother', Starting to wonder if it's a sting ya know." OCE1 responds, "No do you have pic, Yea I don't know."

32. On August 31, 2019, at 1459hrs, Mega user slackermaster2k@yahoo.com posts, "Omg i stopped by Mcdonalds drive thru and was met by the cutest boy with braces brown hair and a whisp of a mustach... right for puberty..i chubbed and wanted to suk him haha,

What a perv."

33. On September 3, 2019, at 0956hrs, OCE1 responds, "[laughing face emoji] I don't blame you!, I love teen fast food workers." At 0957hrs, Mega user slackermaster2k@yahoo.com, responds, "Yes." OCE1 responds, "There tight pants and moist skin, I wish they would cum in my food [Laughing face emoji]." Mega user slackermaster2k@yahoo.com comments, "Usually at eye level with their cock outline." OCE1 responds, "YES!!!!, Haha omg." Mega user slackermaster2k@yahoo.com responds, "I am gonna have to go back for a visit." OCE1 responds, "Good shots of long dicks or ass." Mega user slackermaster2k@yahoo.com responds, "His I think would be smooth or just a whisp of hair." OCE1 responds, "Go back and tip them if you can, That's fine either way, Get to know him!" At 0958hrs, Mega user slackermaster2k@yahoo.com responds, "Yes." Mega user slackermaster2k@yahoo.com then posts an image of a male unclothed from the waist down with an erect penis and no pubic hair. Based on the image, it is hard to determine exact age. OCE1 comments, "Oooo yeah! How old you think he is!" At 1419hrs, Mega user slackermaster2k@yahoo.com responds, "12?, Look at that cock [tongue emoji] [drooling face emoji]." OCE1 responds, "Perfect, Nice smooth little hair good hand and mouth hold [drooling face emoji]." At 1455hrs, Mega user slackermaster2k@yahoo.com responds, "Mmmmmhmmmm."

34. On September 6, 2019, at 0832hrs, Mega user slackermaster2k@yahoo.com posted a Mega link. At 0919hrs, Mega user slackermaster2k@yahoo.com posted an image of

three unclothed teenage boys and an image of a teenage boy with an erect penis. OCE1 comments, "Omg that's a hot boy and dick."

35. On September 15, 2019, at 1854hrs, OCE1 comments, "Hi, Mmm I've got off to that pic so much haha."

36. On September 16, 2019, at 0955hrs, Mega user slackermaster2k@yahoo.com commented, "Yah I leaked hard on him." At 1328hrs, Mega user slackermaster2k@yahoo.com posted another image of what I believe to be the same boy. The image is from a low angle showing the boys erect penis and face. The boy appears to be approximately 13-15 years old.

37. On September 23, 2019, at 0646hrs, Mega user slackermaster2k@yahoo.com posted multiple images of unclothed teenage boys. At 2245hrs, Mega user slackermaster2k@yahoo.com posted an image of an unclothed 14-16 year old boy sitting on a boat motor on a lake. His genitals are covered by his leg.

38. On October 23, 2019, I accessed the Mega link and observed a folder titled "The Goodies" and contained 681 files. The contents were publicly available to anyone with the link. The 35 videos downloaded by OCE1 were still contained in the folder at the time of my download of the entire folder.

39. I reviewed videos that were provided by OCE1 and they were consistent to the full download of the link that I completed. It should be noted that the download only had 674 files. Some examples of titles located in the link are as follows: 2blond 13yo boys Pthc Pedo, Horny 12 yo preteen boy JO and squirts, Swedish 11yo boy(2), and !zzzz Ped

12yo Boy with 16yo Friend-1.

40. Video titled (50) depicts a 4-6 year old male in shorts putting his mouth on a teenage boy's penis, performing oral sex while the teenager is sitting on a couch. This video is 17 seconds long.
41. Video titled (86) reports to be 13 minutes and 6 seconds long. It starts out with a 12-14 year-old male looking into the camera possibly chatting with someone on a computer. The male proceeds to get undressed and starts to masturbate his erect penis. In the corner of the video is the title JackinLads.com
42. Video titled (525) reports to be 25 seconds long. It starts with a 5-6 year old male standing up with his pants down and his erect penis visible. There is an approximately 8-10 year old male with his mouth on the 5-6 year old penis, performing oral sex. The video ends with 3 young males unclothed performing what appears to be anal intercourse on each other.
43. On or about October 18, 2019, a U.S. Department of Justice /FBI administrative subpoena was served upon the New Zealand, DIA, as authorized law enforcement officials for Mega, requesting subscriber and connection log information for the Mega account associated to the email address slackermaster2k@yahoo.com. In response on October 20, 2019, Senior Investigator Jon Peacock, New Zealand, DIA provided information in regards to the account, which included internet protocol logs, device access logs and an account overview.
44. The target slackermaster2k@yahoo.com was first active on the Mega service August 9,

2018, 21:49:47UTC and last accessed this service October 20, 2019, 19:38:16UTC. The user predominately uses an iPhone application to access the Mega service. On June 1, 2019, they report that the Mega user was accessing their account with a computer running Microsoft Windows 10, Microsoft Edge internet browser from their Charter internet account. A sampling of the IP address used to access the Mega services are listed below.

Date / Time	IP Address	Country	Provider
2019-05-23 17:20:31 (UTC)	2600:1008:b106:c5c3:f cf6:7e70:4c70:4791	United States	verizon wireless
2019-06-01 12:17:13 (UTC)	2605:a000:a4c6:5800:a 594:f012:bed1:99da	United States	charter communications
2019-08-18 13:53:04 (UTC)	72.135.115.123	United States	charter communications
2019-08-18 22:57:45 (UTC)	72.135.115.123	United States	charter communications
2019-08-20 18:03:33 (UTC)	174.197.18.91	United States	verizon wireless
2019-08-24 21:58:19 (UTC)	72.135.115.123	United States	charter communications
2019-08-26 22:23:21 (UTC)	72.135.115.123	United States	charter communications
2019-08-27 03:33:02 (UTC)	72.135.115.123	United States	charter communications
2019-08-27 12:11:18 (UTC)	174.198.7.7	United States	verizon wireless
2019-08-30 00:10:50 (UTC)	72.135.115.123	United States	charter communications
2019-09-02 17:26:32 (UTC)	72.135.115.123	United States	charter communications
2019-09-06 11:35:17 (UTC)	72.135.115.123	United States	charter communications
2019-09-07 14:39:37 (UTC)	174.197.2.185	United States	verizon wireless
2019-09-09 10:32:33 (UTC)	72.135.115.123	United States	charter communications
2019-09-10 13:16:29 (UTC)	174.197.12.139	United States	verizon wireless
2019-09-16 13:55:00 (UTC)	174.197.8.190	United States	verizon wireless
2019-09-17 18:11:20 (UTC)	174.197.0.143	United States	verizon wireless
2019-09-20 02:30:47 (UTC)	72.135.115.123	United States	charter communications
2019-09-20 19:00:30 (UTC)	174.198.2.255	United States	verizon wireless
2019-09-21 17:39:40 (UTC)	72.135.115.123	United States	charter communications
2019-09-25 02:29:48 (UTC)	72.135.115.123	United States	charter communications
2019-09-25 03:30:40 (UTC)	72.135.115.123	United States	charter communications
2019-09-28 23:52:40 (UTC)	72.135.115.123	United States	charter communications
2019-09-29 09:40:01 (UTC)	72.135.115.123	United States	charter communications
2019-10-01 22:21:59 (UTC)	72.135.115.123	United States	charter communications
2019-10-03 13:18:49 (UTC)	174.198.5.79	United States	verizon wireless
2019-10-03 23:35:29 (UTC)	72.135.115.123	United States	charter communications
2019-10-04 21:08:32 (UTC)	72.135.115.123	United States	charter communications
2019-10-06 13:59:57 (UTC)	72.135.115.123	United States	charter communications
2019-10-07 19:26:00 (UTC)	174.198.7.215	United States	verizon wireless
2019-10-08 02:34:31 (UTC)	24.208.1.10	United States	charter communications
2019-10-13 12:23:36 (UTC)	24.208.1.10	United States	charter communications
2019-10-14 21:36:28 (UTC)	24.208.1.10	United States	charter communications
2019-10-15 20:56:22 (UTC)	174.197.18.193	United States	verizon wireless
2019-10-16 17:50:25 (UTC)	174.197.6.49	United States	verizon wireless
2019-10-18 11:44:12 (UTC)	174.197.1.202	United States	verizon wireless
2019-10-18 14:15:45 (UTC)	174.197.1.202	United States	verizon wireless
2019-10-18 16:35:41 (UTC)	174.197.1.202 28	United States	verizon wireless
2019-10-18 20:16:52 (UTC)	174.198.43.201	United States	verizon wireless
2019-10-19 02:52:02 (UTC)	24.208.1.10	United States	charter communications
2019-10-19 14:05:10 (UTC)	24.208.1.10	United States	charter communications

45. After review of the IP connections used to access the account, the following IP addresses were subpoenaed for subscriber info:
- 2600:1008:b106:c5c3:fcf6:7e70:4c70:4791, 2605:a000:a4c6:5800:a594:f012:bed1:99da, 72.135.115.123, and 24.208.1.10.
46. IP address 2600:1008:b106:c5ce:fcf6:7e70:4c70:4791 was queried in ARIN and resolved to Cellco Partnership d/b/a Verizon Wireless.
47. IP addresses 2605:a000:a4c6:5800:a594:f012:bed1:99da, 72.135.115.123, and 24.208.1.10 was queried in ARIN (American Registry of Internet Numbers) and resolved to Charter Communications.
48. On or about October 21, 2019, a U.S. Department of Justice /FBI administrative subpoena was served upon Charter Communications requesting subscriber and connection log information associated to 24.208.1.10. In response, on October 25, 2019, Charter Communications advised the subscriber was Mary McKeever at 310 Wyldewood Drive, Oshkosh, Wisconsin. This account was assigned IP address 24.208.1.10 from October 6, 2019 through the date of the subpoena.
49. On or about October 21, 2019, U.S. Department of Justice /FBI administrative subpoena was served upon Charter Communications requesting subscriber and connection log information associated 2605:a000:a4c6:5800:a594:f012:bed1:99da, 72.135.115.123. In response, on October 25, 2019, Charter Communications advised the subscriber was Mary McKeever 610 E. Apple Creek Rd, Appleton, WI for the above listed IP addresses.

50. This would be consistent with the McKeever's moving from Appleton, WI to Oshkosh Wisconsin on or about October 8, 2019.

51. On or about October 21, 2019, a U.S. Department of Justice /FBI administrative subpoena was served upon Cellco Partnership d/b/a Verizon Wireless requesting subscriber and connection log information associated to 2600:1008:b106:c5c3:fcf6:7e70:4c70:479 on May 23, 2019 at 17:20UTC. In response, on October 23, 2019, Cellco Partnership d/b/a Verizon Wireless advised the assigned phone number was 616-402-3381. Cellco Partnership d/b/a Verizon Wireless also advised the subscriber was Martin E McKeever at 310 Wyldewood Drive, Oshkosh, Wisconsin.

52. Based on my training and experience, I believe the IP logs listed above shows that Martin McKeever is utilizing his mobile device which has access to the internet via Verizon cellular connection to access his Mega account. McKeever has distributed child pornography on Mega chat via link files sent to OCE1. It is also my belief that the Mega user slackermaster2k@yahoo.com is Martin McKeever. In the above logs, the Mega account is also being accessed by his Charter internet. Martin McKeever as shown above access his Mega account from both his home internet (Charter) and his mobile phone internet (Verizon). There are also instances of a Microsoft Windows operating system connecting to the Mega account from his home internet. In early October, Martin McKeever moved to his residence in Oshkosh, WI from Appleton WI. It is my belief that he would have brought all of his computers, mobile devices and other items

capable of storing digital media. It would not be normal to leave belonging behind when one moves.

53. On February 27, 2020, OCE2 observed Kik user Alex_Chross joined a private Kik group titled "Babies Only." Since Kik user Alex_Chross joined this group, other users have distributed child pornography including a video of an infant.
54. On March 2 2020, OCE2 asked the Alex_Chross what he was up to and he responded "working". OCE2 asked if they could see what he looked like and he replied by sending a live image of himself. I reviewed the photo that was sent to OCE2 and it is believed to be Martin McKeever after comparing it to his WI Department of Transportation photo.
55. On February 28, 2020, OCE2 observed a video uploaded to the private group described as follows: Prepubescent male approximately 5 to 7 years old with a blindfold over his eyes. An adult male enters the scene and can be seen masturbating his erect penis. The adult male then masturbates to the point of ejaculating into the prepubescent male's mouth. The Kik user Alex_Chross then commented on that video stating "Good boy." Based on this comment, it is believed that he viewed this video.
56. On February 28, 2020, OCE2 began a private conversation with Kik user Alex_Chross. During this conversation, Kik user Alex_Chross informed OCE2, that he was from Oshkosh, Wisconsin. Kik user Alex_Chross was asked if he was into young and he replied "not really babies like em a bit older." Kik user Alex_Chross was asked what ages he preferred, and he replied "yeah i was thinking like 9 or 10+ just about to bud

or starting they are so cute like that." During the private conversation with OCE2, Kik user Alex_Chross disclosed that he designed vehicles for a manufacturing unit and then clarified and said trucks.

57. On February 28, 2020, at 1427hrs, Kik user Alex_Chross stated, "no no its fine in a meeting rn.... chat shortly," "meetings suck on fridays I should be at happy hour."
58. On November 5, 2019, FBI SA Sarah Deamron conducted surveillance at the above address and did observe the following vehicle parked in the garage at the address. White Honda CR-V, Wisconsin License Plate 635-MUW, which is registered to Mary Ann McKeever.
59. On February 7, 2020, a Google search for Martin McKeever revealed a LinkedIn profile featuring a picture of Martin McKeever. The LinkedIn profile states he is an Associate Design Engineer for Oshkosh Corporation.
60. On March 2, 2020, a query of property records with the City of Oshkosh Assessment Services Division revealed 310 Wylewood Drive, Oshkosh, Wisconsin is owned by Martin E McKeever and Mary A McKeever since October 7, 2019.
61. The target residence, 310 Wylewood Drive is located on a private drive off of Wyldewood Drive. There is a sign at the entrance for "The Villas of Wyldewood." On the sign, it lists what addresses are on the private drive and "310" is listed.
62. On March 3, 2020, SA Robert Rice was conducting surveillance with other members of the FBI surveillance team in the area of 310 Wyldewood Drive, Oshkosh, WI. At 0530hrs, a light was observed on at the residence. At 0545hrs, a white 4 door car

Wisconsin registration plate 848-TBB exited off the private road that is used to access the residence at 310 Wyldewood Drive. The vehicle was followed to Oshkosh Global Systems Center on 33rd Ave Oshkosh WI.

63. Immediately after the vehicle was observed SA Robert Rice drove by the residence and observed what he described as the garage door open light on, which he could see through the glass on the garage door. He did not observe any other garage door lights on in the area.

64. On March 3, 2020, I conducted a search of the Wisconsin Department of Transportation (WI DOT) records on the following people and vehicle. Martin E. McKeever M/W DOB: 06/25/69 and Mary Ann McKeever F/W DOB: 01/25/63. WI DOT reported that they both list 310 Wyldewood Drive, Oshkosh, WI as their address. WI Vehicle registration plate 848-TBB was submitted to WI DOT and listed Martin McKeever as the owner at 310 Wyldewood Dr. Oshkosh, WI.

65. Based on this investigation, I believe Martin McKeever resides at 310 Wyldewood Drive, Oshkosh and from that residence has accessed KIK to view child pornography. Kik is traditionally utilized on a portable device running IOS (apple product) operating system or android operating system, which includes tablets and phones or other devices capable of running those operating systems. Kik can be used on a traditional windows computer if a special program is used to emulate an android operating system. The program runs and allows android application such as Kik to be used on the computer and function properly. Further, I believe he has distributed child

pornography or links to child pornography using his phone or computer while at his former residence in Appleton. I believe his current residence will have evidence of this distribution in the form of the actual child pornography videos or movie files posted or evidence in the form of devices he used to post those files. Furthermore, Mckeever utilized MEGA which can be accessed on a mobile device or a web browser. The web browser may be on a portable device or traditional computer or laptop. Mega can be used for cloud storage or chatting. These devices could hold identifying information specifically the email account slackermaster2k@yahoo.com or evidence of access to that account. Portable devices may be used to access child pornography but the user can easily connect to storage devices or computers and move the files to those mediums for easier viewing and larger storage capacities.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS CHILD
PORNOGRAPHY

66. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web based bulletin boards to access with intent to view images of child pornography:
67. Individuals who possess child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such

as in person, in photographs, or other visual media; or from literature describing such activity.

68. Individuals who possess child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
69. Individuals who possess child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
70. Likewise, individuals who possess child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cell phone. These collections are often maintained for several years and are kept close by, usually at the collector’s residence or inside the collector’s vehicle, to enable the individual to view the collection, which is valued highly.

71. Individuals who possess child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
72. Individuals who would have knowledge about how to access a hidden and embedded bulletin board would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.
73. Individuals who possess child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
74. Based on the following, I believe that a user of the Internet account at SUBJECT PREMISES, likely displays characteristics common to individuals who access with the intent to view and/or, possess, collect, receive, or distribute child pornography.
75. I have been involved with investigations with individuals who have been convicted of

crimes against children in the past and have re offended.

BACKGROUND ON ELECTRONIC STORAGE DEVICES
AND CHILD PORNOGRAPHY

76. Computers, cellular telephones, and other electronic storage devices (collectively electronic storage devices) have dramatically changed the way in which individuals interested in child pornography interact with each other. Electronic storage devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
77. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a device by simply connecting the camera to the electronic storage device. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the video recorder to a computer. Many electronic storage devices (e.g., computers, cellular telephones, and tablets), have cameras built

into the device which allows users to create and store still and video images on the device. Moreover, if the device has internet connectivity, users can distribute still and video images from the device.

78. Internet-enabled electronic storage devices can connect to other internet-enabled devices the world over. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to an internet-enabled electronic storage device. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, electronic storage devices are the preferred method of distribution and receipt of child pornographic materials.

79. Electronic storage devices are the ideal repository for child pornography. The amount of information that an electronic storage device can hold has grown exponentially over the last decade. Electronic storage devices can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on a computer or other electronic storage device. It is extremely easy for an individual to

take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Many electronic storage devices can easily be concealed and carried on an individual's person.

80. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
81. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any internet-enabled electronic storage device. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's electronic storage device in most cases.
82. As is the case with most digital technology, communications by way of electronic storage device can be saved or stored on the device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client

software, among others). In addition to electronic communications, an electronic storage device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

83. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, I believe the images/videos described in paragraphs 31 through 61 above are still located in and can be retrieved from the electronic storage devices at the SUBJECT PREMISES.

84. Your affiant is requesting a search warrant for: 310 Wyldewood Drive, Oshkosh, Wisconsin, and Any Person(S) found Therein or Thereon and any Outbuilding at the above location. Authorization to Seize, and forensically or manually search items described in **Attachment (B)**.

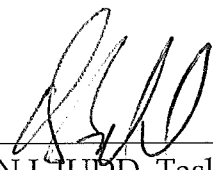
85. Further, I am seeking authorization to conduct this search outside of the 6:00 am to 10:00 pm time period. My investigation shows that Mr. McKeever departs from his residence for work prior to 6:00 am. I am seeking permission to execute this search

warrant while Mr. McKeever is in his residence so that he is not at work and in a position to flee or destroy evidence that would be located either during the search or in other remote storage locations.

86. Believing said searches will produce evidence of the crime of Receipt, Transportation, and Distribution, and Conspiracy to Receive, Transport, and Distribute, Child Pornography, contrary to 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1); and Possession and Access, or Attempted Access, with Intent to View Child Pornography contrary to 18 U.S.C. § 2252A(a)(5)(B) and (b)(2).

87. Based on the above, I submit that this affidavit supports probable cause for a warrant to search the premises described in Attachment A and seize and then search the items described in Attachment B.

Dated this 5th day of March 2020.



BRIAN J. JUDD, Task Force Officer
Federal Bureau of Investigation

Sworn to before me this 5th day of March 2020.



Honorable James R. Sickel
United States Magistrate Judge

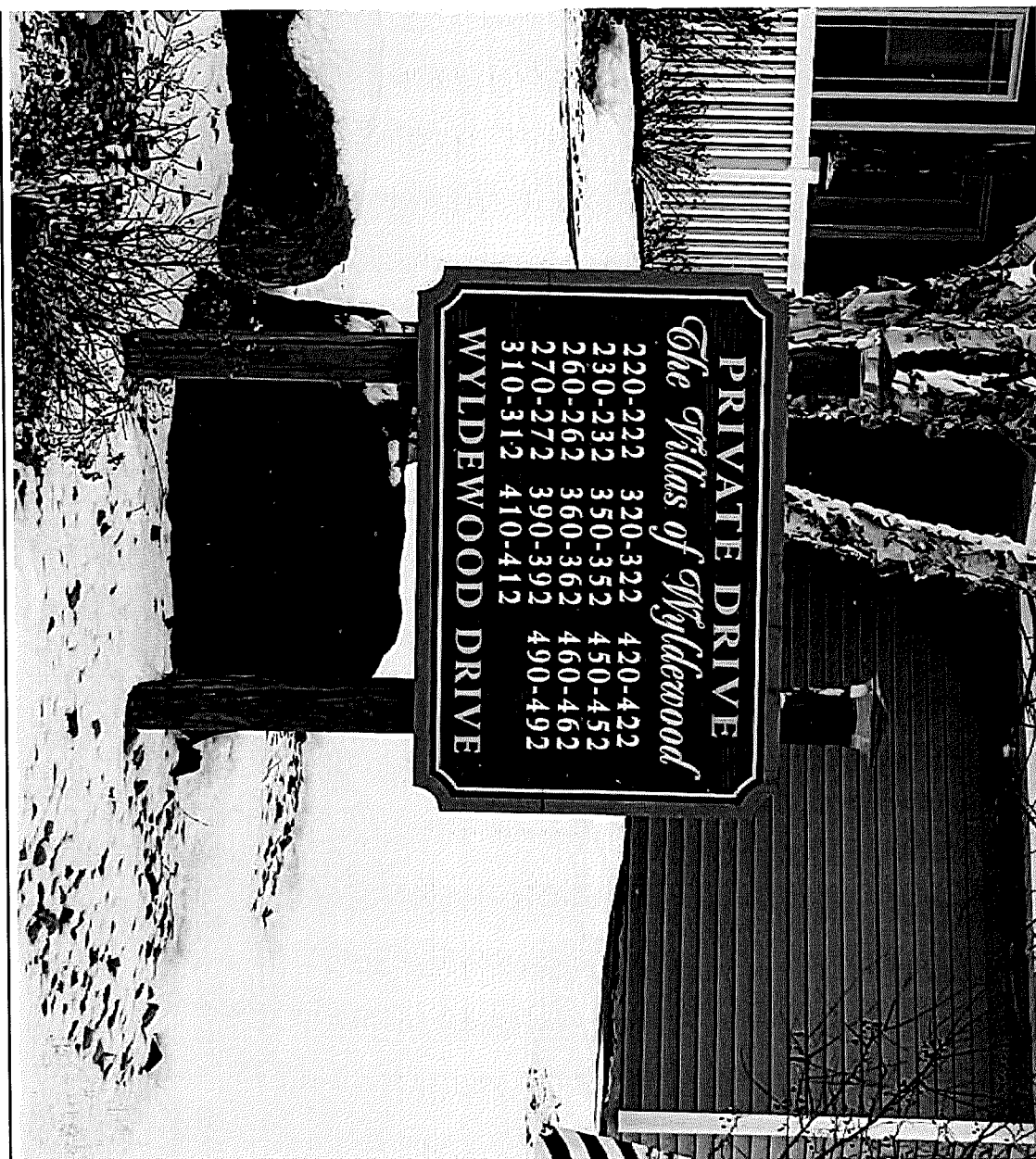
ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as **310 Wyldewood Dr, Oshkosh, Wisconsin** is identified as follows: Side by side duplex with light tan siding and dark brown shingles, white trim with a two car garage. The address tile which is affixed to the right side of the garage displays “310”. The residence is located on a Private Drive and the property is called “The Villas of Wyldewood”







ATTACHMENT B

1. All records relating to violations of Title 18, United States Code, Sections 2252A, derived from the search of the subject premises and further search of computers, cell phones and other devices located therein including:
 - a. Records containing child pornography or pertaining to the distribution, receipt or possession of child pornography;
 - b. Records evidencing occupancy or ownership of the premises described above, including but not limited to utility and telephone bills, mail envelopes, or addressed correspondence;
 - c. Cellular telephones, telephone and address books, and other notes and papers insofar as they memorialize, include, or confirm computer screen names, contact information, or images related to the sexual exploitation of children, in violation of Title 18, United States Code, Section 2252A;
 - d. Any and all records of any form or other items or materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence, including but not limited to sales receipts, invoices, bills for Internet access, and handwritten notes.
2. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the lack of such malicious software;
- d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. Evidence of the times the COMPUTER was used;
- g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. Contextual information necessary to understand the evidence described in this attachment;
 - i. Routers, modems, and network equipment used to connect computers to the Internet;

- ii. Records of Internet Protocol addresses used;
- iii. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet or P2P search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).